AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A method of generating electronic keys d for a public-key cryptography method using an electronic device, comprising the following two separate calculation steps:

Step A

1) calculating pairs of prime numbers (p, q) or values representative of pairs of prime numbers, this calculation being independent of knowledge of a pair of values (e, l) in which e is the public exponent and l is the length of the key of the cryptography method,

2) storing the pairs or values thus obtained in a memory of a secure electronic object; and

Step B

obtaining values for e and l;

retrieving a pair of prime numbers (p, q), or a value representative of said pair of prime numbers, stored in step A;

verifying the following conditions for said pair of prime numbers:

(i) p-1 and q-1 are prime numbers with the obtained value for e and

(ii) N=p*q is an integer of given length l,

if the pair (p, q) does not satisfy conditions (i) and (ii), retrieving another pair of prime numbers and repeating the verification until a retrieved pair is suitable; and calculating a key d to be used by the secure electronic object from the retrieved pair (p, q) that is determined to be suitable.

2. (Previously Presented) The method of Claim 1, wherein step A-1) comprises calculating pairs of prime numbers (p, q) without knowledge of the public exponent e or of the length l of the key, using a parameter Π which is the product of small prime numbers, so that each pair (p, q) has a maximum probability of being able to correspond to a future pair (e, l) and can make it possible to calculate the key d.

3. (Previously Presented) The method of Claim 2, wherein the calculation of step A-1) also takes account of the fact that e has a high probability of forming part of the set {3, 17, ..., $2^{16}+1$}, and using a seed σ in the calculation which makes it possible to calculate a representative value constituting an image of the pairs (p, q).

4. (Previously Presented) The method of claim 3, wherein the storage step A-2) comprises storing the image of the pairs.

5. (Previously Presented) The method of Claim 2, wherein step A-1) comprises calculating pairs of prime numbers (p, q) for different probable pairs of values (e, l).

6. (Previously Presented) The method of claim 5, wherein the parameter Π contains the values 3, 17.

7. (Previously Presented) The method of Claim 1, wherein step A-1) comprises an operation of compressing the calculated pairs (p, q) and step A-2) comprises storing the compressed values thus obtained.

8. (Previously Presented) The method of Claim 3, wherein step A-1) comprises the generation of a prime number q for which a lower limit B_0 is set for the length l_0 of this prime number that is to be generated, such that $l_0 \geq B_0$, and further comprising the following sub-steps:

1) calculating parameters v and w from the following relations and storing them:

$$v = \sqrt{2^{2\ell_0-1}} / \Pi$$

$$w = 2^{\ell_0} / \Pi$$

in which Π is stored and corresponds to the product of the f smallest prime numbers, f being selected such that $\Pi \leq 2^{B_0}$,

2) selecting a number j within the range of integers {v, ..., w-1} and calculating $l = j\,\Pi$;

3) selecting and storing a prime number k of short length compared to the length of an RSA key within the range of integers {0, ..., Π-1}, (k, Π) being co-prime;

4) calculating q=k+l,

5) verifying that q is a prime number, if q is not a prime number then:

a) taking a new value for k using the following relation:

k = a k (mod Π); a belonging to the multiplicative group Z^*_Π of integers modulo Π;

b) repeating the method from step 4).

9. (Previously Presented) The method of claim 8, wherein the numbers j and k can be generated from the seed σ stored in memory.

10. (Previously Presented) The method of Claim 8, wherein the prime number p is generated by repeating all the above sub-steps while replacing q with p and replacing l_0 with l-l_0.

11. (Canceled)

12. (Currently Amended) A secure portable object able to generate electronic keys d of an RSA-type cryptography algorithm, comprising:

communication means for receiving at least one pair of values (e, l),

a memory for storing results of calculating pairs of prime numbers (p, q) or values representative of pairs of prime numbers, this calculation being independent of knowledge of the pair of values (e, l) in which e is a public exponent and l is the length of the key of the cryptography method; and

a program for calculating a key d from the stored results and knowledge of a received pair of values (e, l);

wherein the program comprises instructions that cause a processor to perform the following operations to calculate the key d:

retrieve a pair of prime numbers (p, q), or a value representative of said pair of prime numbers, stored in the memory;

verify the following conditions for said pair of prime numbers:

(i) p-1 and q-1 are prime numbers with the obtained value for e and

(ii) N=p*q is an integer of given length l,

if the pair (p, q) does not satisfy conditions (i) and (ii), retrieve another pair of prime numbers stored in the memory and repeat the verification until a retrieved pair is suitable; and

calculate the key d from the retrieved pair (p, q) that is determined to be suitable.

13. (Previously Presented) The secure portable object according to Claim 12, further comprising a calculation means configured to calculate said results stored in memory, the calculation of said results being separate in time from the calculation of the key d.

14. (Previously Presented) The secure portable object according to Claim 13, wherein the calculation means is configured to carry out the following sub-steps:

1) calculating parameters v and w from the following relations and storing them:

$$v = \sqrt{}2^{2\ell_0-1} / \Pi$$

$$w = 2^{\ell_0} / \Pi$$

in which Π is stored and corresponds to the product of the f smallest prime numbers, f being selected such that $\Pi \leq 2^{B_0}$, and B_0 is a lower limit set for the length l_0 of the prime number that is to be generated, such that $l_0 \geq B_0$,

2) selecting a number j within the range of integers {v, ..., w-1} and calculating l=j Π;

3) selecting and storing a prime number k of short length compared to the length of an RSA key within the range of integers {0, ..., Π-1}, (k, Π) being co-prime;

4) calculating q=k+l,

5) verifying that q is a prime number, if q is not a prime number then:

a) taking a new value for k using the following relation:

k = a k (mod Π); a belonging to the multiplicative group Z^*_Π of integers modulo Π; and

b) repeating the method from step 4).

15. (Previously Presented) The secure portable object according to Claim 12 wherein said object is a chip card.

16. (Previously Presented) The method of Claim 1, wherein step A-1) comprises calculating pairs of prime numbers (p, q) for different probable pairs of values (e, l).

17. (Previously Presented) The method of Claim 1, wherein step A-1) comprises the generation of a prime number q for which a lower limit B_0 is set for the

length l_0 of this prime number that is to be generated, such that $l_0 \geq B_0$, and further comprising the following sub-steps:

1) calculating parameters v and w from the following relations and storing them:

$v = \sqrt{2^{2\ell_0-1}} / \Pi$

$w = 2^{\ell_0} / \Pi$

in which Π is stored and corresponds to the product of the f smallest prime numbers, f being selected such that $\Pi \leq 2^{B_0}$,

2) selecting a number j within the range of integers {v, ..., w-1} and calculating $l = j\,\Pi$;

3) selecting and storing a prime number k of short length compared to the length of an RSA key within the range of integers {0, ..., Π-1}, (k, Π) being co-prime;

4) calculating q=k+l,

5) verifying that q is a prime number, if q is not a prime number then:

a) taking a new value for k using the following relation:

k = a k (mod Π); a belonging to the multiplicative group Z^*_Π of integers modulo Π;

b) repeating the method from step 4).

18. (Previously Presented) The method of Claim 17, wherein the prime number p is generated by repeating all the above sub-steps while replacing q with p and replacing l_0 with l-l_0.

19. (Previously Presented) A method of generating an electronic key for a public-key cryptography method in an electronic device, which key has a length l and is based upon a public exponent e, comprising the following steps:

- in a computing resource external to said electronic device:

calculating pairs of prime numbers (p, q), or values representative of said pairs of prime numbers, independently of the values for e and l, and

storing the pairs of prime numbers, or values, in a memory of the electronic device;

- in said electronic device:

obtaining values for e and l;

retrieving a pair of prime numbers (p, q), or a value representative of said pair of prime numbers, from said memory;

verifying the following conditions for said pair of prime numbers:

(i) p-1 and q-1 are prime numbers with respect to the value for e, and

(ii) N=p*q is an integer of length l,

if the pair (p, q) does not satisfy conditions (i) and (ii), retrieving another pair of prime numbers from said memory and repeating the verification steps until a retrieved pair is determined to meet the conditions; and

calculating a key d in accordance with the value for e and a retrieved pair that is determined to meet the conditions.